

UNITED STATES DISTRICT COURT

for the
Southern District of West Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

1616 Spring Valley Drive, Apt. 5,
Huntington, WV 25704

Case No. 3:17-mj-00023

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Southern District of West Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 USC 2423(b) and (e) Travel to Engage in Illicit Sexual Misconduct

The application is based on these facts:

See attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Cedric Jefferson, FBI SA

Printed name and title

Sworn to before me and signed pursuant to Rule 4.1 of the FRC Proc.

Date: June 8, 2018


Judge's signature

City and state: Beckley, WV

Omar J. Aboulhosn, United States Magistrate Judge

Printed name and title

ATTACHMENT A

- 1) **Description of Location to be Searched:** The premises at **1616 Spring Valley Drive, Apartment 5, Huntington, WV 25704**—further described as a two-story apartment residence in the Park Place apartment complex, depicted below. The entrance to Apartment 5 is indicated by the blue arrow (below)—the door on the right.



ATTACHMENT B

- 1) The property to be searched is **a cellular telephone associated with telephone number 304-377-0052**, belonging to STEVEN MICHAEL PURSELL of 1616 Spring Valley Drive, Apartment 5, Huntington, WV, including any memory cards (“SIM”) that are in the telephone (hereafter referred to as “Subject Telephone”).
- 2) This warrant authorizes the forensic examination of the Subject Telephone for the purpose of identifying the following electronically stored information:
 - a. All records, information, and items on Subject Telephone that relate to violations of Title 18, United States Code, Sections 2251(a), 2252(a)(4)(b), and 2423(b) and involve STEVEN MICHAEL PURSELL since March 1, 2017, including:
 - i. incoming and outgoing call and text message logs;
 - ii. contact lists;
 - iii. photo and video galleries;
 - iv. sent and received text messages;
 - v. online searches and sites viewed via the internet;
 - vi. online or electronic communications sent and received, including email, chat, and instant messages;
 - vii. sent and received audio files;
 - viii. navigation, mapping, and GPS files;
 - ix. telephone settings, including speed dial numbers and the telephone number for the subject telephone and related identifying information such as the ESN for the telephone;
 - x. messages drafted but not sent;

- xi. voice messages;
- b. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. However, no real-time communications will be intercepted and searched during service.

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH WARRANT

I, Cedric Jefferson, Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), assigned to the Charleston, West Virginia, Resident Agency Office of the Pittsburgh Division. I have been employed as a Special Agent for the FBI since January 2015. I am currently tasked with investigating violations of federal law within the Southern District of West Virginia and elsewhere. As part of my duties, I have received training regarding the investigation of various federal crimes including, but not limited to, child exploitation, complex financial crimes, and violent crimes. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. As a Special Agent, I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7).

2. I know that Title 18, United States Code, Section 2251(a) makes it a crime to produce material depicting the sexual exploitation of a minor (child pornography) and that Section 2252(a)(4)(B), makes it a crime to possess child pornography.

3. I also know that Title 18, United States Code, Section 2423(b) makes it a crime to travel for the purpose of engaging in illicit sexual conduct with a child. The term “illicit sexual conduct” is defined in 18 U.S.C. § 2423(f) as “as sexual act . . . with a person under 18 years of age that would be in violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction of the United states.” A violation of 18 U.S.C. § 2243(a)(1) (Chapter 109A) occurs when an adult person knowingly engages in a sexual act with a child who has

attained the age of 12 years old but is less than 16 years old, and the adult is at least four years older than the child.

4. As a federal agent, your affiant is authorized to investigate violations of the laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

5. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at located at **1616 Spring Valley Drive, Apartment 5, Huntington, WV**, for the person of the STEVEN MICHAEL PURSELL who resides at the premises, further described in Attachment A, and for the vehicle belonging to STEVEN MICHAEL PURSELL. This application seeks authority for a warrant to search for, seize, and forensically evaluate the items identified in Attachment B, which I submit constitute evidence, fruits, and instrumentalities of violations of, among other statutes: Title 18, United States Code, Sections 2250, 2251(a), 2252(a) and 2423—offenses involving the sexual exploitation of children and child pornography.

6. The statements in this affidavit are based on my training, experience, and information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of a violations of Title 18, United States Code, Sections 2251(a), 2252(a)(4)(b), and 2423(b), is presently located at **1616 Spring Valley Drive, Apartment 5, Huntington, WV**, the person of STEVEN MICHAEL PURSELL, and/or in the vehicle associated with the target premises and/or STEVEN MICHAEL PURSELL, as further described in Attachment A.

**BACKGROUND ON COMPUTERS, CELLULAR TELEPHONES, AND CHILD
EXPLOITATION**

7. Based on your Affiant's training, experience, and knowledge, your Affiant knows the following:

a. Computers, computer technology, and cellular telephones have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. The development of computers and mobile devices (e.g., smartphones, tablets) has added to the methods used by child pornography collectors/producers interact with and sexually exploit children. With the advance of technology, the distinction between computers and cellular telephones is quickly becoming less clear. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic address books; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; accessing and downloading information from the Internet, and using maps and getting directions from one location to another. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Computers and mobile devices serve four functions in connection with child pornography; production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs directly from a camera or mobile device to a computer storage system. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection.

Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem, or via mobile devices. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, the computer and Internet-capable mobile devices are preferred methods of distribution and receipt of child pornographic materials.

d. The advent of webcams and cellular phones with built-in cameras has enabled child pornographers to broadcast live transmissions of sexual abuse of minors by easily connecting the webcam or camera to the Internet. A webcam is a video camera that attaches to a computer or that is built into a laptop or desktop screen. The software included with webcams also permits an individual to capture and save live transmissions to the computer or peripheral storage devices. A webcam can be used in conjunction with an instant messaging service which permits real-time, direct, text-based communication between two or more people while permitting the individuals to view each other real-time via the webcam. However, a webcam is not required in order to receive live transmissions of activity that is taking place in front of another user’s webcam. The same can be accomplished using a cellular telephone with a built-in camera. Such cellular telephones can record still images or video, allowing the user to share the images and/or video in real time using direct, text-based communications between two people or more or, where the phone is also a “smart phone” with Internet access, a user can upload the images or videos taken with the phone’s built-in camera to the Internet or a social media website.

e. The ability of a computer or mobile device to store images in digital form makes these devices an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text, and CDs, DVDs, and flash drives can store hundreds of images and thousands of pages of text. The size of the electronic storage media (commonly referred to as the hard drive or thumb drive) used in home computers has grown tremendously within the last several years. Electronic storage devices with the capacity of 750 gigabytes are common, and electronic storage devices in excess of one terabyte (1,000 gigabytes) are now available for sale for low cost. These drives can store thousands of images at very high resolution. It is possible to use digital cameras and “video” cameras (designed primarily to record moving images), including those contained in mobile devices such as cellular telephones, to upload images to the Internet. Only through careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail generated by this activity.

f. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

g. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography in various formats, including services offered by Internet Portals such as Microsoft Live, Yahoo!, Google, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or electronic device such as a phone, tablet, or other device with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer and/or mobile devices, in most cases.

h. As is the case with most digital technology, communications by way of computer and mobile device can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files, cache, or ISP client software, among others). In addition to electronic communications, a computer or mobile device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. For example, computers often indefinitely retain archived conversations from instant messaging programs as well as messaging logs and files shared over instant messaging.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

8. Computer hardware, software, electronic files and data security devices (such as passwords) may be important to a criminal investigation in two distinct ways: (1) the items themselves may be evidence of, or contraband, fruits, or instrumentalities of a crime; and/or (2) the items may have been used to collect and store information about crimes in an electronic or digital format. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize items that are evidence of, contraband, fruits, or instrumentalities of crime. I believe that in this case, the cellular telephone located at the subject premises, on the person of STEVEN MICHAEL PURSELL, and/or in a vehicle listed in this affidavit, is a container for evidence and fruits of a crime, and is itself an instrumentality of the crime under investigation since this cellular phone was used to produce/attempt to produce child pornography.

9. Searches and seizures of evidence from computers/mobile devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following reasons:

a. The volume of evidence. Computer storage devices, including mobile phones, can store the equivalent of thousands of pages of information. Additionally, when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names or extensions. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days, weeks, or even months depending on the volume of data stored, and it would be impractical to attempt this kind of data search on-site.

b. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional tampering or destruction (which may be caused

by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

c. Time factors. It is possible for computer experts to recover files or remnants of files, even months or years after they have been deleted, but doing so requires a significant investment of time. The ability to retrieve residue of an electronic file is time consuming and depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits. As previously mentioned, the size of electronic storage media used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 500 gigabytes and more are common.

d. The computer media itself. In order to fully retrieve data from a computer system, the analyst needs all or most of a computer system's equipment, and may be required to seize hardware, peripherals, software, documentation, security devices and passwords. In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

10. Furthermore, because there is probable cause to believe that the computer and its storage devices, in this case—a cellular telephone and any memory cards ("SIM") contained therein, are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

11. The property to be searched is a **cellular telephone associated with telephone number 304-377-0052, belonging to STEVEN MICHAEL PURSELL of 1616 Spring Valley Drive, Apartment 5, Huntington, WV**, including any memory cards (“SIM”) that are in the telephone (hereafter referred to as “Subject Telephone”). As detailed herein, there is probable cause to conclude that the Subject Telephone contains evidence of the commission of federal felony offenses.

12. The applied-for warrant would authorize the forensic examination of the Subject Telephone for the purpose of identifying electronically stored data particularly described in Attachment B.

SEARCH METHODOLOGY TO BE EMPLOYED

13. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;
- b. examination of all of the data contained in such computer hardware, computer software, or memory storage devices, including cell phones, to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth

herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- d. surveying various file directories and the individual files they contain;
- e. opening files in order to determine their contents;
- f. scanning storage areas;
- g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

PROBABLE CAUSE

14. On or about March 24, 2017, Minor A's mother contacted Pennsylvania State Police (PSP) Trooper First Class (TFC) Joshua K. Thomas regarding her fourteen-year-old daughter, Minor A, having had sexual contact with a thirty-four-year-old male. Minor A admitted to her mother that on March 20, 2017, sometime before midnight, she snuck out of her home at 129 Esther Drive, Hookstown, Pennsylvania to meet an adult male who she had met on the Internet social media site Facebook approximately one month ago. The two then traveled to a Super 8 hotel in the Moon Township area of Allegheny County, Pennsylvania where they had unprotected sexual intercourse at the hotel. The adult then transported Minor A back to her residence at approximately 4:00 AM the next day.

15. TFC Thomas was able to determine that Minor A and the adult went to the Super 8 hotel located at 8991 University Boulevard, Coraopolis, PA 15108. Super 8 hotel employees confirmed that an adult male by the name of STEVEN MICHAEL PURSELL checked into the hotel shortly before midnight on March 20, 2017 and checked out shortly after 9:00 AM on March 21, 2017. TFC Thomas obtained the following documentation from the Super 8 hotel in Coraopolis, PA with regard to room rented by PURSELL on March 20, 2017: (i) a registration form signed by STEVEN PURSELL, (ii) a photo copy of PURSELL'S West Virginia driver's license, (iii) PURSELL'S U.S. Department of Veteran's Affairs identification card, and PURSELL'S USAA Visa credit card. Super 8 hotel employees also provided footage from the hotel's video surveillance that shows PURSELL checking into the hotel and entering the lobby area of the hotel with Minor A on March 20, 2017.

16. According to Minor A, her date of birth is March 8, 2003. TFC Thomas determined through law enforcement databases that PURSELL's date of birth is July 28, 1982, and that he has a West Virginia driver's license listing the address of 84 Victorian Commons, Winfield, WV.

17. On May 5, 2017, the United States Postal Inspection Service provided information that on March 19, 2017 a mail forwarding request was filed for STEVEN PURSELL directing that any mail addressed to STEVEN PURSELL at the 84 Victorian Commons, Winfield, WV address be forwarded to STEVEN PURSELL at **1616 Spring Valley Drive, Apartment 5, Huntington, WV.**

18. On March 28, 2017, TFC Thomas interviewed Minor A at the PSP Beaver Barracks. During the interview, Minor A relayed the following: Minor A met PURSELL on the Internet social media site, Facebook, approximately one month prior to their physical meeting on March 20, 2017. They met when PURSELL sent Minor A a Facebook friend request. Thereafter,

they used Facebook Messenger and video calling to communicate. Minor A accessed Facebook from the laptop that was supplied to her by her school. Minor A stated that she and PURSELL communicated exclusively on Facebook and almost every day. She stated that their conversations routinely were sexual in nature. Specifically, they talked about Minor A and PURSELL having sex. Minor A informed PURSELL that she was fourteen years old. According to Minor A, when she told PURSELL that she was fourteen years old “it didn’t faze him.” On Monday, March 20, 2017, PURSELL made plans with Minor A to travel to Western Pennsylvania, pick Minor A up at her home, and take her to a hotel to have sex. Minor A gave PURSELL her home address and, that same day, PURSELL traveled to Western Pennsylvania and followed through with their plans—he picked Minor A up at an intersection near her home and transported her in his vehicle to the Super 8 hotel in Coraopolis, PA.

19. Minor A reported that PURSELL picked her up some time before midnight. Minor A confirmed that the person in the vehicle that picked her up was in fact the person with whom she had been communicating via Facebook over the previous month. She described the individual as a white male, heavy build, dark hair and a tattoo of “Chinese characters” on his forearm. While the two traveled to the hotel, PURSELL told Minor A: “I’m risking a lot for you.” Upon arriving at the hotel, PURSELL told Minor A to remain in the vehicle while he went into the lobby of the hotel. After PURSELL returned to the vehicle, he directed Minor A to walk ahead of him into the hotel. This was confirmed by video provided by the hotel.

20. Minor A went with PURSELL into room 311 of the Super 8 hotel. Minor A related that upon entering the room, she went into the bathroom to change. PURCELL entered the bathroom while she was changing, and began kissing her. When PURSELL exited the bathroom, Minor A began to shave her legs and pubic area. PURSELL then reentered the bathroom and held

his phone in such a way that Minor A believed PURSELL was video recording and/or taking photographs of Minor A shaving her legs and pubic area. When Minor A exited the bathroom, PURSELL picked her up and placed her on the bed where he pulled down the top of her dress, exposing Minor A's breasts. She felt uncomfortable and pulled the dress back up over her chest. She stated that this happened multiple times. Ultimately, PURSELL placed his mouth on Minor A's bare breasts. PURSELL also performed oral sex on Minor A and had unprotected vaginal sex with her until he ejaculated inside her.

21. Minor A also described how PURSELL used men's neck ties to bind her. She described how the ties were placed around her head and across her mouth as a gag, and that this binding attached to another that bound her hands and feet. Minor A described the position as being "hog tied." While Minor A was bound, PURSELL touched her around her vaginal area and put his fingers inside of her vagina. PURSELL removed the bindings when Minor A told him that they hurt her. After PURSELL removed the bindings, he began manipulating his cell phone and then showed Minor A his cell phone screen, which was set to video mode. Minor A described the video as still running and stated that she saw a comment on PURSELL's cell phone screen from an unknown individual stating: "She doesn't look 18." Minor A described the video as a "live stream" and recalled seeing other comments on the screen. PURSELL then told her: "I made \$5." PURSELL then set up his cell phone in a position such that it could record their sexual activity on the bed. While PURSELL's cell phone was set up in this manner, Minor A performed oral sex on PURSELL and PURSELL again had vaginal sex with Minor A to the point of ejaculation.

22. At approximately 4:00 AM, PURSELL drove Minor A home in his personal vehicle. PURSELL then told Minor A not to contact him anymore and subsequently blocked her on Facebook. On or about March 24, 2017, Minor A told a friend about her interactions with

PURSELL. The friend then told Minor A's mother about it, prompting Minor A's mother to confront Minor A about it. At that point Minor A told her mother about her interactions with PURSELL.

23. Verizon Wireless confirmed for law enforcement that since at least January 15, 2017, Steven PURSELL is the subscriber of a cellular telephone associated with the telephone number **304-377-0052**. The associated service address for subscriber PURSELL is **1616 Spring Valley Dr., Apartment 5, Huntington, WV**.

24. The Super 8 registration form that TFC Thomas obtained from the Super 8 hotel with PURSELL's signature also had the number PURSELL provided at registration: 304-377-0042. This phone number is one digit off from the cellular telephone number associated with PURSELL, as confirmed by Verizon.

25. On June 2, 2017, law enforcement received information from West Virginia's Department of Health and Human Resources, Child Protective Service about an individual named STEVEN PURSELL with an address of **1616 Spring Valley Drive, Huntington, WV** and a telephone number of **304-377-0052**.


26. Law enforcement checked with West Virginia's Department of Motor Vehicles and found that the following vehicle is associated with the target premises and/or STEVEN MICHAEL PURSELL: **2015 Chevrolet Malibu, WV license plate OZZ469**, dark brown in color.

27. Based on my training and experience, I know that cellular technology and mobile computing devices are highly portable, and may be easily stored or concealed on the person of the user/owner. They may also be stored or concealed in a vehicle and, in fact, are commonly found in vehicles.

CONCLUSION

28. Considering all of the foregoing, probable cause exists that STEVEN MICHAEL PURSELL committed violations of Title 18, United States Code, Sections 2251(a), 2252(a)(4)(b), and 2423(b). There is also probable cause to believe that evidence of these crimes will be found at the target premises, on the person of PURSELL who resides at the premises, and/or in the vehicle belonging to PURSELL. Your Affiant respectfully requests that this Court issue a search warrant for the subject device described in Attachment A and for items listed in Attachment B.

Further your affiant sayeth naught.


CEDRIC JEFFERSON
Special Agent
Federal Bureau of Investigation

Sworn to in my presence by telephonic means and subscribed, this 8th day of June, 2017.


OMAR J. ABOULHOSN
UNITED STATES MAGISTRATE JUDGE

Executed pursuant to Rule 4.1 of the Federal
Rules of Criminal Procedure